UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA v. SERGEY ALEYNIKOV, Defendant.	10 CR. 0096 (DLC) ECF Case

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS THE INDICTMENT

MARINO, TORTORELLA & BOYLE, P.C.
437 Southern Boulevard
Chatham, New Jersey 07928-1488
(973) 824-9300
Attorneys for Defendant Sergey Aleynikov

On the Brief:
Kevin H. Marino
John D. Tortorella
John A. Boyle
Roseann Bassler Dal Pra

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Regulations

Journals & Treatises

Other Authorities

PRELIMINARY STATEMENT

Defendant Sergey Aleynikov ("Aleynikov") respectfully submits this memorandum of law in support of his motion to dismiss the Indictment pursuant to Federal Rule of Criminal Procedure 12(b)(3)(B) for failure to state an offense under any of the three federal criminal statutes it invokes: the Economic Espionage Act of 1996 (the "EEA"); the Interstate Transportation of Stolen Property Act (the "ITSPA"); and the Computer Fraud and Abuse Act (the "CFAA").

This is not a motion to dismiss the Indictment for failure to provide sufficient particulars to apprise the defendant of the charges against him. The Indictment is certainly specific enough to apprise Aleynikov of the essential elements of the three statutes the grand jury alleges he violated and to inform him and the Court of how the grand jury alleges he violated those statutes — specifically, by accessing, downloading and transporting computer source code for Goldman Sachs & Company's ("Goldman") high-frequency trading business. Rather, this is a motion to dismiss the Indictment because the specific facts it alleges — and the facts implied by those specific allegations — clearly fall beyond the scope of the charged statutes as a matter of statutory interpretation. As the Indictment fails to state an offense, it must be dismissed.

Each count of the Indictment proceeds from the factual allegation that before leaving his employment at Goldman, Aleynikov copied the firm's proprietary computer source code for its high-frequency trading business with the intent to injure Goldman and to benefit himself and his new employer, Teza Technologies, LLC ("Teza"). Count One alleges that Aleynikov's source code copying violated the EEA, which criminalizes theft of a trade secret "related to or included in a product that was produced for or placed in interstate or foreign commerce." Count Two

alleges that because Aleynikov subsequently carried the copied computer source code across state lines, he violated the ITSPA, which prohibits the interstate transfer of stolen "goods, wares, merchandise, securities, and money." Count Three alleges that because Aleynikov obtained the computer source code by copying it from a Goldman computer, his copying of the code violated the CFAA, which penalizes one who accesses a computer without authorization or who exceeds authorized access to obtain information.

These factual allegations make clear that the Indictment is fatally defective because the acts of which Aleynikov stands accused — copying, transporting and accessing proprietary computer source code for an investment bank's high-frequency trading business — do not constitute the federal crimes for which he was indicted. His conduct does not transgress the EEA, as Count One alleges, because "proprietary computer source code for Goldman's high-frequency trading business" is not "a trade secret ***related to or included in a product that was produced for or placed in interstate or foreign commerce.***" To the contrary, as the Indictment makes clear, the purported ***"product"*** that source code is ***"related to or included in"*** is a proprietary system of computer programs and trading algorithms that Goldman has not licensed and has not otherwise made available to the public. By its very terms, the Indictment confirms that the ***"product"*** the trade secret ***"is related to or included in"*** was neither "***produced for"*** nor ***"placed in"*** either ***"interstate*** or ***foreign commerce."*** Thus, whatever else might be said of it, what the Indictment alleges is a ***"product"*** — a proprietary system of computer programs and trading algorithms that Goldman was and is determined to keep secret — is certainly not, as the statute requires, a ***"product that was produced for or placed in interstate or foreign commerce."*** Count One must therefore be dismissed.

Nor did Aleynikov's alleged transportation of Goldman's proprietary computer source code across state lines violate the ITSPA, as Count Two alleges. Just as a secret system of computer programs and trading algorithms is not "a product that was produced for or placed in interstate or foreign commerce," proprietary computer source code does not constitute ***"goods, wares, merchandise, securities, or money"*** as the ITSPA requires. To the contrary, such computer source code is classic intellectual property, excluded by its very nature from the reach of a statute proscribing the theft of five specifically-identified categories of personal property. Count Two must therefore be dismissed.

Finally, Aleynikov did not violate the CFAA by accessing the Goldman computer from which he copied its source code, as Count Three alleges, because (a) the Indictment concedes that he was authorized to access that computer and computer code; and (b) the CFAA does not prohibit an employee's misappropriation of information to which the employee was given access and which the employee lawfully obtained. Count Three must therefore be dismissed.

For the reasons outlined above and amplified below, the Indictment must be dismissed in its entirety for failure to state an offense.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

A. Background.[1]

1. Goldman.

Goldman provides financial services in the United States and around the world and is engaged in, among other financial activities, high-frequency trading on various commodities and equities markets. (Indictment, ¶ 1.) High-frequency trading is a type of trading activity carried out in various financial markets that allow orders to buy and sell to be placed electronically. (Id., ¶ 4.) Typically, high-frequency trading involves the extremely rapid execution of high volumes of trades in which trading decisions are made by sophisticated computer programs that use complex mathematical formulas, known as algorithms. (Id.) Those algorithms make trading decisions based on statistical analysis of past trades and moment-to-moment developments in the markets. (Id.)

Goldman's high-frequency trading business was supported by a system of computer programs, which the Government refers to as the "Platform," which, inter alia, rapidly obtained information regarding the latest market movements and trends, processed that information into a form that could be analyzed by Goldman's trading algorithms, and then executed the trading decisions produced by the algorithms. (Id., ¶ 5.) The Platform gave Goldman a competitive edge with respect to its trades. (Id.)

Since in or around 1999, Goldman has employed computer programmers to develop and maintain both the Platform and Goldman's trading algorithms. (Id., ¶ 6.) The computer

[1] The background facts are derived from the Indictment and are accepted as true for purposes of this motion. United States v. Kerik, 615 F. Supp. 2d 256, 260 (S.D.N.Y. 2009).

programmers developed and modified the programs constituting Goldman's high-frequency trading system by writing and altering the "source code" of those programs. (Id., ¶ 7.) Source code is a series of instructions that specify the actions to be performed by a computer program. (Id.) According to the Indictment, "Goldman has not licensed its trading algorithms or the Platform, and has not otherwise made them available to the Public." (Id., ¶ 6.)

2. Aleynikov

From in or around May 2007 through June 5, 2009, Aleynikov was employed by Goldman as a Vice President in its Equities Division. (Indictment, ¶¶ 9, 10.) Throughout that time, Aleynikov was a member of the team of computer programmers responsible for developing and improving certain aspects of the Platform. (Id., ¶ 9.)

In late April 2009, Aleynikov accepted a position with Teza, a startup company based in Chicago, as Executive Vice President, Platform Engineering. (Id., ¶ 10.) In that position, Aleynikov, among other Teza employees, was to be responsible for developing Teza's own high-frequency trading business that would compete with Goldman's business. (Id.)

3. The Alleged Theft of Goldman's High-Frequency Trading Source Code.

On many occasions prior to his last day of work at Goldman, Aleynikov transferred, without Goldman's approval and in violation of Goldman's policies, source code for Goldman's high-frequency trading system to his home computers, including a laptop computer. (Id., ¶ 14.) Upon his termination of employment, Aleynikov did not return to Goldman any of the source code for its high-frequency trading system, in violation of his confidentiality agreement with Goldman. (Id.)

On June 5, 2009, the last day on which Aleynikov worked in Goldman's offices, he

transferred hundreds of thousands of lines of source code for Goldman's high-frequency trading system from its computer network, including files relating to the Platform and the trading algorithms, to a server in Germany. (Id., ¶ 12.) The server was associated with a website that offered services to computer programmers who wished to store their source code projects. (Id., ¶ 12(b). Thereafter, Aleynikov accessed the website from his home in New Jersey and downloaded the source code files to his home computer. Several days later, he copied some of the files to other home computers and to a portable flash drive. (Id., ¶ 13.)

On July 2, 2009, Aleynikov flew to Chicago to attend meetings at Teza's offices. (Id., ¶ 15.) Aleynikov brought his laptop computer and flash drive, which contained source code for Goldman's high-frequency trading system, including some of Goldman's source code files that he had copied and transferred. (Id.) The Indictment does not allege that Aleynikov transferred or offered to transfer any source code to Teza at that meeting or at any other time.

On the evening of July 3, 2009, a team of FBI agents arrested Aleynikov when his flight from Chicago landed at Newark's Liberty International Airport.

B. The Indictment.

1. Count One (Economic Espionage Act of 1996)

In Count One, the Indictment charges Aleynikov with violating, attempting to violate, and aiding and abetting a violation of, the EEA. The statutory allegations in this count state:

> From at least in or about May 2009, up to and including on or about July 3, 2009, in the Southern District of New York and elsewhere, SERGEY ALEYNIKOV, the defendant, unlawfully, willfully, and knowingly, without authorization copied, duplicated, sketched, drew, photographed, downloaded, uploaded, altered, destroyed, photocopied, replicated, transmitted, delivered, sent, mailed, communicated, and conveyed a trade secret, as that term is

> defined in Title 18, United States Code, Section 1839(3), and attempted so to do, with intent to convert such trade secret, that was related to and included in a product that was produced for and placed in interstate and foreign commerce, to the economic benefit of someone other than the owner thereof, and intending and knowing that the offense would injure the owner of that trade secret, to wit, ALEYNIKOV, while in New York, New York and elsewhere, without authorization copied and transmitted to his home computer Goldman's proprietary computer source code for Goldman's high-frequency trading business, with the intent to use that source code for the economic benefit of himself and his new employer, Teza.

(Indictment, Count One, citing 18 U.S.C. §§ 1832(a)(2), 1832(a)(4) and (2).)

2. Count Two (Interstate Transportation of Stolen Property Act)

Count Two of the Indictment charged Aleynikov with violating and aiding and abetting a violation of the ITSPA. The statutory allegations in this count state:

> From in or about June 2009, up to and including in or about July 2009, in the Southern District of New York and elsewhere, SERGEY ALEYNIKOV, the defendant, unlawfully, willfully, and knowingly, transported, transmitted, and transferred in interstate and foreign commerce goods, wares, merchandise, securities, and money, of the value of $5,000 and more, knowing the same to have been stolen, converted and taken by fraud, to wit, ALEYNIKOV, while in New York, New York, copied, without authorization, Goldman's proprietary computer source code for Goldman's high-frequency trading business, the value of which exceeded $5,000, uploaded the code to a computer server in Germany, and carried that stolen code to a meeting with his new employer, Teza, in Chicago, Illinois.

(Indictment, ¶ 18 (citing 18 U.S.C. § 2314 & 2).)

3. Count Three (Computer Fraud and Abuse Act)

Count Three, the final count of the Indictment, charges Aleynikov with violating and aiding and abetting a violation of the CFAA. The statutory allegations in this count state:

> In or about June 2009, in the Southern District of New York and elsewhere, SERGEY ALEYNIKOV, the defendant, unlawfully, intentionally, and knowingly, and, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States and of any State, accessed a protected computer without authorization and exceeded authorized access, which computer was used in and affecting interstate and foreign commerce and communication, and thereby obtained information from such protected computer the value of which exceeded $5,000, to wit, ALEYNIKOV, while in New York, New York, in violation of Goldman's policies and his confidentiality agreement with Goldman, accessed a computer server maintained by Goldman and copied Goldman's proprietary computer source code for Goldman's high-frequency trading business, the value of which exceeded $5,000, uploaded the code to a computer server in Germany, and then downloaded it to his home computer, all with the intent to use that source code for the economic benefit of himself and his new employer, Teza.

(Indictment, ¶ 20 (citing 18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i-iii) and 2).)

Because the facts alleged do not state a violation of the charged statutes, this motion to dismiss the Indictment follows.

LEGAL ARGUMENT

I. LEGAL STANDARD.

Aleynikov moves to dismiss the Indictment pursuant to Fed. R. Crim. P. 12(b)(3)(B) for failure to state an offense. Rule 12(b)(3)(B) provides, in pertinent part, that "at any time while the case is pending, the court may hear a claim that the indictment . . . fails . . . to state an offense." Id. "[A] charging document fails to state an offense if the specific facts alleged in the charging document fall beyond the scope of the relevant criminal statute, as a matter of statutory interpretation." United States v. Panarella, 277 F.3d 678, 685 (3d Cir. 2002); see also United States v. Russell, 639 F. Supp. 2d 226, 236 (D. Conn. 2007) (noting that it would be proper to

dismiss an indictment that fails to state an offense under the charged statute); United States v. Sunia, 643 F. Supp. 2d 51, 68 (D.D.C. 2009) (dismissing indictment where facts it alleged did not constitute crime charged as a matter of statutory construction); United States v. Thompson, No. CR-09-88-FVS, 2010 U.S. Dist. LEXIS 41005, at *2 (E.D. Wash. Apr. 27, 2010) (noting that an indictment "fails to state an offense" if the specific facts alleged in it fall beyond the scope of the relevant criminal statute as a matter of statutory interpretation).

In Panarella, the Court held that, "for purposes of Rule 12(b)(2),[2] a charging document fails to state an offense if the specific facts alleged in the charging document fall beyond the scope of the relevant criminal statute, as a matter of statutory interpretation." Id. The Panarella court made that straightforward statement of the law in response to the Government's argument that "an indictment or information charges an offense, for purposes of Rule 12(b)(2), as long as it recites in general terms the essential elements of the offense, ***even if the specific facts alleged in the charging instrument fail to satisfy those elements.***" Panarella, 277 F.3d at 685 (emphasis supplied).

Panarella's common sense rejection of the Government's argument — that an indictment that tracks the language of a criminal statute states an offense even where the facts it alleges do not fall within the meaning of that statute — is consistent with the law of this and every other circuit with respect to the sufficiency of an indictment. As your Honor noted in United States v. Kim, No. 09 Cr. 1160, 2010 U.S. Dist. LEXIS 43454, at *5 (S.D.N.Y. May 4, 2010), "an

[2] The Federal Rules of Criminal Procedure were amended effective December 1, 2002. The new Rule 12 places the old Rule 12(b)(2), which authorizes the filing of a motion to dismiss an indictment or information for failure to state an offense, at Rule 12(b)(3)(B). Thus, although cases decided prior to that date refer to Rule 12(b)(2) as the rule permitting such motions, that rule now appears at Rule 12(b)(3)(B).

indictment need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime." Id. (quoting United States v. Yannotti, 541 F.3d 112, 127 (2d Cir. 2008) and citing United States v. De La Pava, 268 F.3d 157, 162 (2d Cir. 2001)); see also United States v. Walsh, 194 F.3d 37, 44 (2d. Cir. 1999) (quoting United States v. Tramunti, 513 F.2d 1087, 1113 (2d Cir. 1975)). Specifically, an indictment "need only allege 'the "core of criminality" the government intend[s] to prove' at trial, and consequently . . . is 'read . . . to include facts which are necessarily implied by the specific allegations made.'" Kim, 2010 U.S. Dist. LEXIS 43454, at *6 (S.D.N.Y. May 4, 2010) (quoting United States v. Rigas, 490 F.3d 208, 229 (2d Cir. 2007)); see also United States v. Rankin, 870 F.2d 109, 112 (3d Cir. 1989); United States v. American Waste Fibers Co., 809 F.2d 1044, 1046 (4th Cir. 1987); United States v. Adkinson, 135 F.3d 1363, 1375 n.37 (11th Cir. 1998). But an indictment is certainly defective — under the law of this and every other circuit — when its factual allegations, however broadly and generously interpreted, allege conduct that simply does not violate the charged statutes.

In United States v. Pacione, 738 F.2d 567, 573 (2d Cir. 1984), for example, the defendant moved to dismiss those counts of an indictment that charged him with violating the extortionate credit statute, 18 U.S.C. § 891 *et seq.*, by threatening to record a mortgage and a deed. Id. at 569. Although the indictment tracked the language of the statute, the defense argued that the threat of non-violent conduct it alleged as a factual basis for that statutory violation "was not what congress meant to prohibit in the extortionate credit statute." Id. at 569. Judge Knapp granted the motion, agreeing with the defense that those facts did not establish a violation of the statute. Id. Rejecting the Government's appeal, the Second Circuit affirmed that dismissal

because its analysis of the statute revealed that, as Judge Knapp had concluded, the defendant's activities as alleged in the indictment were beyond the limits of that statute. Id. at 572.

To similar effect was the First Circuit's decision in United States v. Rosa-Ortiz, 348 F.3d 33 (1st Cir. 2003), which affirmed the dismissal of an indictment charging the defendant with conspiracy to violate the Federal Escape Act, 18 U.S.C. § 751(a), because that statute does not prohibit the conduct charged in the indictment. In Rosa-Ortiz, the indictment charged the defendant with conspiring to violate § 751(a) by assisting in the escape of his co-defendant, who was in federal custody on a federal material witness warrant. The defendant pleaded guilty to that charge and appealed, arguing that his conduct was not within the crime charged. The First Circuit agreed, finding that § 751(a), which by its terms proscribes escapes of those in federal custody "by virtue of an arrest on a charge of felony, or conviction of any offense," does not apply to the escape of one taken into federal custody on a material witness warrant. The court explained, "[t]he plain text of [§ 751(a)] does not support the indictment in this case, and 'due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope.'" Id. at 42 (quoting United States v. Lanier, 520 U.S. 259, 266 (1997)).

The approach taken by the Second Circuit in Pacione and the First Circuit in Rosa-Ortiz is reflective of that taken by numerous district courts throughout the country. See, e.g., United States v. Gray, 101 F. Supp. 2d 580, 588 (E.D. Tenn. 2000) (dismissing count of indictment because it alleged a course of conduct involving multiple financial transactions, an offense the court held 18 U.S.C. § 1956(a)(1)(B)(i) did not criminalize); United States v. Pees, 645 F. Supp. 697, 704 (D. Col. 1986) (dismissing indictment alleging that defendant distributed a Schedule I

substance, in violation of 18 U.S.C. § 846, where the drug charged in the offense had not been properly classified under Schedule I); United States v. Ashford, 403 F. Supp. 461, 464-65 (N.D. Iowa 1975) (dismissing charge that defendant violated 18 U.S.C. § 1708 for failure to state an offense because an essential element was that a letter had been stolen or embezzled while "in the mail," but the indictment charged that the letter in question was addressed "care of" the defendant, who subsequently formed the intention to steal it); United States v. Murillo, No. 07 Cr. 2026, 2008 U.S. Dist. LEXIS 19568, at *8 (N.D. Iowa Mar. 13, 2008) (dismissing charge for failure to state a cause of action because the social security card defendant was alleged to have used did not constitute a "means of identification" within the meaning of 18 U.S.C. § 1546(b)).

As these cases make clear, an indictment that tracks the language of a charged statute and conveys the relevant core of criminality ***but alleges facts that do not violate the statute it charges*** cannot be sustained. The fatal flaw in such indictments is not that they fail to allege the charge with sufficient specificity, but rather that the facts they allege make clear that the charge cannot be maintained. As the Eleventh Circuit explained in United States v. Peter, 310 F.3d 709 (11th Cir. 2002):

> The problem is not that the Government's case left unanswered a question as to whether its evidence would encompass a particular fact or element. Rather, it is that the Government affirmatively alleged a specific course of conduct that is outside the reach of the mail fraud statute. Peter's innocence of the charged offense appears from the very allegations made in the superseding information, not from the omission of an allegation requisite to liability.

Id. at 715.

That is precisely the problem in this case. Each count of the Indictment charges Aleynikov with a different crime, and each parrots the language of a different statute, arising

from his alleged copying of proprietary computer source code for Goldman's high-frequency trading business. But none of the counts alleges facts that would under any circumstances bring Aleynikov's conduct within the meaning of the charged statutes. Charging that the computer source code he copied was related to Goldman's high-frequency trading business does not — and never will — state the offense of stealing a trade secret "related to or included in a product produced for or placed in interstate or foreign commerce" under the EEA because a secret high-frequency trading business is not a product produced for or placed in interstate or foreign commerce within the meaning of that statute. Charging that the computer source code Aleynikov copied was transported from state to state does not state the offense of transporting a stolen "good, ware, merchandise, securities or money" under the ITSPA because proprietary computer source code does not constitute a good, ware, merchandise, securities or money within the meaning of that statute. Charging that Aleynikov accessed the Goldman computer from which he copied its source code does not state the offense of exceeding authorized access under the CFAA because the Indictment itself charges that he ***was*** authorized to access that computer and computer code, and such authorized access does not transgress the CFAA. For these reasons, the Indictment is defective and must be dismissed.

II. THE FIRST COUNT FAILS TO STATE AN OFFENSE UNDER THE EEA BECAUSE THE TRADE SECRET IT ALLEGES WAS STOLEN WAS NEITHER RELATED TO NOR INCLUDED IN A PRODUCT THAT WAS PRODUCED FOR OR PLACED IN INTERSTATE OR FOREIGN COMMERCE.

Count One charges Aleynikov with theft of a trade secret, as well as attempted theft of a trade secret and aiding and abetting theft of a trade secret, under the EEA. That statute provides, in pertinent part:

> (a) Whoever, with intent to convert ***a trade secret, that is related to***

> ***or included in a product that is produced for or placed in interstate or foreign commerce***, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly –
>
> . . . .
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information[]
>
> . . . .
>
> (4) attempts to commit any offense described in paragraphs (1) through (3)[] shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years.

18 U.S.C. § 1832(a) (emphasis supplied). As the statutory language makes clear, and as the Department of Justice (the "DOJ") has recognized in its Intellectual Property Manual, to establish a violation of the EEA the Government must prove, inter alia, that the trade secret was "'related to or included in ***a product that is produced for or placed in interstate or foreign commerce***.'" United States Department of Justice, Prosecuting Intellectual Property Crimes 160-61 (3d ed. 2006) ("IP Manual") (quoting 18 U.S.C. § 1832)) (emphasis added).

Here, the Indictment charges that the trade secret Aleynikov allegedly stole is related to "Goldman's high-frequency trading business" (Indictment, ¶ 16), which the Indictment alternately refers to as "Goldman's high-frequency trading system" (id., ¶ 7) and the "Platform" (id., ¶ 5). (For ease of reference, all three terms are referred to herein as the Platform.)[3] That the

[3] In most of its allegations the Indictment describes the Platform as the entirety of Goldman's high-frequency trading business (Indictment, ¶¶ 5, 6, 9, 12), but in a few instances it instead refers to "Goldman's high-frequency trading system" and suggests that the "trading system" includes components, such as trading algorithms, in addition to the Platform. (See, e.g., Indictment, ¶ 7 ("At all times relevant to this Indictment, Goldman's high-frequency trading system — the Platform and the trading algorithms —

Platform is the "product" that, according to the grand jury, was "related to or included in" the trade secret Aleynikov copied is made plain in the Indictment itself, which is replete with references to the Platform, its purported value to Goldman and its confidential and proprietary nature, including the following: (1) "ALEYNIKOV, while in New York, New York and elsewhere, without authorization copied and transmitted to his home computer Goldman's proprietary computer source code for ***Goldman's high-frequency trading business***" (id., ¶ 16); (2) "Goldman's high-frequency trading was supported by ***a proprietary system of computer programs (the 'Platform')***" (id., ¶ 5); (3) "[t]he rapid speed at which ***the Platform*** could perform these tasks conferred a competitive advantage to Goldman with respect to its trades" (id.); (4) "Goldman has not license ***its trading algorithms or the Platform*** and has not otherwise made them available to the public" (id., ¶ 6); (5) "At various times relevant to this Indictment, Goldman has taken various measures to protect ***its high-frequency trading system's source code***" (id., ¶ 8); (6) "Throughout his employment at Goldman, ALEYNIKOV was a member of a team of computer programmers responsible for developing and improving certain aspects of ***the Platform***" (id., ¶ 9); (7) "during his employment at Goldman, ALEYNIKOV worked on source code related to ***the Platform's*** connection to NASDAQ" (id.); (8) "[i]f ALEYNIKOV simply executed the 'backup' program without entering the additional command, it would copy [ ] very many of the source code files for ***the Platform and for some of Goldman's trading algorithms***"

---

were comprised of [sic] different computer programs."); see also id., ¶¶ 14, 15.) The "Statutory Allegations" section in turn alleges that the code copied by Aleynikov was part of the "high frequency trading business" (Id., ¶ 16). Regardless of whether the Government alleges that the Platform is a component of the high-frequency trading system (rather than the system itself) or that the trading system and the Platform are part of Goldman's high-frequency trading business, the arguments made herein with respect to the deficiencies in the Indictment's EEA charge apply with equal force.

(id., ¶ 12(a)); and (9) ALEYNIKOV brought with him [to Teza in Chicago] both the Laptop Computer and the Flash Drive, which, at that time, each contained source code for ***Goldman's high-frequency trading system***" (id., ¶ 15).

The core of criminality alleged in the Indictment thus could not be clearer: Aleynikov stole a trade secret — specifically, proprietary computer source code — included in or related to Goldman's high-frequency trading platform with the intent to use that source code to develop a competing trading platform at Teza. But the EEA does not proscribe such conduct. To the contrary, the EEA proscribes the theft of a trade secret that is included in or related to ***a product that is produced for or placed in interstate or foreign commerce***. The statute is obviously designed to criminalize the act of stealing a trade secret embodied in a product that is produced for if not actually placed in the stream of commerce. Goldman's high-frequency trading Platform does not meet that description by anyone's lights. The Platform is not a "product" as that term is commonly understood and used, either in legal settings generally or for purposes of the EEA specifically, and the Platform was not produced for or placed in interstate or foreign commerce. Rather, according to the Indictment, the Platform is a secret trading system, internal to Goldman and destined to remain there, never to see the light of day. A federal criminal statute that by its express terms proscribes the theft of intellectual property included in or related to a product bound for or placed in the stream of commerce does not proscribe the theft of a trade secret related to or included in Goldman's high-frequency trading Platform.

A. The Platform Does Not Constitute A "Product."

Because it is not a tangible item of personal property distributed to and used by the commercial public, the Platform does not constitute a product. Black's Law Dictionary defines a

"product" as "[s]omething that ***is distributed commercially*** for use or consumption and that is usu[ally] (1) ***tangible personal property***, (2) the result of fabrication or processing, and (3) an item that has ***passed through a chain of commercial distribution*** before ultimate use or consumption." Black's Law Dictionary 1245 (8th ed. 2004) (emphasis added). Judge Karas adopted that definition of "product" in a case involving contractual interpretation. Cacae v. Meyer Mktg. (Macau Commercial Offshore) Co., Ltd., 589 F. Supp. 2d 314, 321 & n.3 (S.D.N.Y. 2008) (referring to dictionary definition of the word "product" as the ordinary English language usage of the term and quoting the entirety of the definition in Black's Law Dictionary); see also KN Energy v. Rockwell Int'l Corp., 840 F. Supp. 95, 99 (D. Colo. 1993) (applying the Black's Law Dictionary's definition of "consumer product"[4] in the context of the Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. § 9601, et seq.).

Likewise, section 19 of the Restatement (Third) Torts: Product Liability provides that "[a] product is ***tangible*** personal property ***distributed commercially*** for use and consumption." (emphasis added). Judge Chin relied on Section 19 in Gorran v. Atkins Nutritionals, Inc., 464 F. Supp. 2d 315 (S.D.N.Y. 2006), which adopted that section's definition of a "product" in holding that the intangible expressions in a diet book did not constitute a product for strict product-liability purposes. Id. at 324-25. Section 19's definition of a "product" has also been adopted by federal courts in settings outside the product liability context. See, e.g., United States v. Brown, 348 F.3d 1200, 1213 (10th Cir. 2003) (adopting Section 19's definition of "product" to find

[4] Black's Law Dictionary defined "consumer product" at the time as ***"[a]ny tangible personal property which is distributed in commerce*** and which is normally used for personal, family, or household purposes . . ." KN Energy, 840 F. Supp. at 99 (quoting Black's Law Dictionary 317 (6th ed. 1990)).

inapplicable an income tax exemption that applied to refunds related to products sold in the ordinary course of business). Further, in at least one instance — the Magnuson-Moss Warranty Act (15 U.S.C. § 2301, et seq.) — Congress has expressly defined "product" in words virtually identical to those found in the Restatement. 15 U.S.C. § 2301(1) ("The term 'consumer product' means ***any tangible personal property which is distributed in commerce*** and which is normally used for personal, family, or household purposes (including any such property intended to be attached to or installed in any real property without regard to whether it is so attached or installed).") (emphasis added).

These authorities all make clear that for an item to constitute a "product," it must have two hallmark characteristics: (1) it must be tangible personal property; and (2) it must be distributed commercially for use and consumption by the public. Thus, in Saloomey v. Jeppesen & Co., 707 F.2d 671 (2d Cir. 1983), the Second Circuit held that navigational charts constituted a product, rather than a service, for the imposition of strict product liability because the charts were mass produced and marketed for commercial distribution. Id. at 677. In so holding, the court contrasted mass produced, marketed and commercially distributed navigational maps with the "mere provision of architectural design plans or any similar form of data supplied under individually-tailored service arrangements." Id.

Similarly, in Anastasio v. Kahn, No. 09 Civ. 5213, 2010 U.S. Dist. LEXIS 2661 (E.D. Pa. Jan. 13, 2010), the district court, relying on the principles and definitions set forth in the Restatement, dismissed products liability claims arising out of an accident in a supermarket parking lot on the ground that the lot owner was not the "seller" of a "product." Id. at **6-8. In so holding, the court explained that the concept of a "seller" "involves the 'transfer of possession

of the subject product.'" Id. at *7 (quoting Voelker v. United Airlines, Inc., No 93 Civ. 1653, 1993 U.S. Dist. LEXIS 13130 at *2 (E.D. Pa. July 6, 1993)). Consistent with the principle that an item must be distributed to qualify as a "product," the court explained:

> The Voelker court held that United Airlines was not a seller and therefore was not subject to a claim of strict liability under Section 402A, insofar as it was "not in the business of transferring the possession of aircraft in any way." Id. Likewise, the court in [Greenwood v. Busch Entm't Corp, 101 F. Supp. 2d 292, 295 (E.D. Pa. 2000),] held that an amusement park could not be strictly liable for injuries caused by a water slide because "there was no relinquishment of control or possession of [the slide] to [plaintiff]." 101 F. Supp. 2d at 295. In support of its holding, Greenwood cited a comment to Section 20 of the Third Restatement of Torts, entitled "Definition Of 'One Who Sells Or Otherwise Distributes,'" which states "[i]f the product is not used up or consumed, the transaction is usually not treated as a sale of a product, but rather as a service." 101 F. Supp. 2d at 295 (citing Restatement (Third) of Torts: Prods. Liab. § 20 Reporters' Note, cmt. d).

Anastasio, 2010 U.S. Dist. LEXIS 2661, at *7-8.

In another context, the court in General Dynamics Corp. v. United States, 202 Ct. Cl. 347 (1973), also focused on the fact that an item was not sold or otherwise commercially distributed in determining that it was not a product. The issue in General Dynamics was whether certain "selling" costs associated with an experimental prototype aircraft were reimbursable under a procurement contract with the government. Id. at 361-62. One of the threshold questions for reimbursement was the existence of a product. Id. at 362-63. As to that issue, the court concluded that the Armed Services Board of Contract Appeals (whose opinion the court was considering on appeal) had correctly held that the prototype aircraft was not a product within the meaning of the governing procurement regulations because "it was an experimental aircraft built to demonstrate its general STOL capabilities." Id. at 361. Stated differently, because the aircraft

was not intended for commercial distribution and sale, but rather simply to evidence that the aircraft would meet required performance specifications, it did not fall within the commonly accepted definition of a "product."

The above cases and legal authorities demonstrate that for an item to constitute a "product" it must be tangible personal property distributed commercially for use and consumption by the general public. This general, ordinary definition of a product is equally applicable in the context of the Economic Espionage Act. See Flores-Figueroa v. United States, 129 S. Ct. 1886, 1891 (2009) ("The manner in which courts ordinarily interpret criminal statutes is fully consistent with th[e] ordinary English usage."). In fact, the legislative history of the EEA evinces that Congress, when it enacted the statute, was specifically concerned with trade secrets relating to commercially distributed products. As the Third Circuit noted shortly after passage of the EEA, the statute became law "against a backdrop of increasing threats to corporate security and a rising tide of international and domestic economic espionage." United States v. Hsu, 155 F.3d 189, 194 (3d Cir. 1998). At the time, foreign governments were actively targeting U.S. persons, firms, industries and the U.S. Government itself to steal critical information to provide "their own industrial sectors with a competitive advantage." S. Rep. No. 104-359, 1996 WL 497065 (Leg. Hist.), at *7 (quotation marks omitted). At the same time, U.S. companies also faced the threat of theft by insiders. Id. In Senate Report No. 104-359, Congress cited several disturbing examples of how thefts were occurring. Id. at **8-9. Significantly, each example involved the theft of trade secrets relating to items that were commercially distributed for use and consumption by members of the public, including air bags, microchips, software, MRI machines, and pharmaceuticals; none of the examples provided by Congress related to items, like

Goldman's high-frequency trading Platform, that were not sold, licensed, leased or otherwise distributed to the commercial public. Id.

In keeping with this legislative history and uniform legal authority interpreting the term "product," the DOJ has itself acknowledged that, for purposes of an EEA prosecution, the alleged product must be a tangible item that is commercially distributed. Specifically, in discussing the EEA's "product" element, the DOJ's IP Manual instructs that "[t]o prove that the product was produced for interstate or foreign commerce, the government need only show the victim's ***intent to distribute the product*** or utilize the process under development for a product." IP Manual at 160-61. Elsewhere, the DOJ opines that "technical skills and know-how" will only constitute a product when included in "***a saleable, transportable*** good." Id. at 161 (emphasis added). Simply put, the DOJ recognizes that the "product" element of an EEA charge requires a saleable, transportable item of tangible personal property that is distributed or intended for distribution in commerce.

Likewise, the U.S. Attorneys' Manual ascribes the above ordinary meaning to the term "product" as used in the EEA. Specifically, in discussing the "product" element of an EEA violation, the U.S. Attorneys' Manual instructs that "[i]n cases where the trade secret is related to a product actually being ***manufactured and sold***, this element is easily established by evidence of ***interstate sales***." United States Department of Justice, United States Attorneys' Manual, § 9-59.100 (emphasis supplied). The Government's manual goes on to counsel that "in cases in which the trade secret is related to a product still being developed but that product ***will ultimately be sold*** in interstate commerce, prosecutors should establish this fact, and argue that it sufficiently meets this element." Id. (emphasis added).

The Government's internal analysis of the EEA's requirement that the stolen trade secret by "related to or included in a product that was produced for or placed in interstate or foreign commerce" is particularly persuasive, for it provides the best insight into what the Government itself thinks about that requirement when it is instructing prosecutors on how to enforce the law rather than when it is trying to salvage a defective indictment. The DOJ and United States Attorneys' Manuals make clear that where the victim's product embodying the stolen trade secret has been finalized and put on the market, the EEA's "included in a product that was placed in interstate or foreign commerce" language applies. Where, on the other hand, the trade secret is stolen while the victim's product is still in development — and thus is not yet embodied in a product on the market — the EEA's "related to a product that was produced for" language applies. So interpreted, the EEA is an effective tool for deterring and punishing the theft of proprietary information related to the products a manufacturer develops for sale regardless of whether that theft occurs before the product in question has actually been finalized and placed in the stream of commerce. It does not apply, however, to the theft of a trade secret that is neither included in a product already on the market nor related to one that is being produced for the market.

Not surprisingly, a review of cases brought to date under the EEA reflects a focus on trade secrets relating to tangible products actually sold, licensed or otherwise distributed. See United States v. Yang, 281 F.3d 534, 540, 551 (6th Cir. 2002) (patent application related to a new adhesive product produced and sold in the United States and Canada); United States v. Lange, 312 F.3d 263, 264-65 (7th Cir. 2002) (computer data used by a company in the business of making aircraft parts for the aftermarket to make a brake assembly); United States v. Martin,

228 F.3d 1, 6, 10-13 (1st Cir. 2000) (trade secrets related to diagnostic test kits for pets and livestock); United States v. Shiah, No. SA CR 06-92, 2008 U.S. Dist. LEXIS 11973, at **2, 39, 46, 55 (C.D. Cal. Feb. 19, 2008) (documents at issue contained information related to products sold by a semiconductor company to international PC manufacturers); United States v. Case, 656 F. Supp. 2d 603, 606, 607 (S.D. Miss. 2009) (trade secrets consisted of technology related to the design, specifications, manufacture and sale of military and commercial aviation hydraulics); United States v. Williams, 526 F.3d 1312 (11th Cir. 2008) (trade secrets belonging to Coca Cola Company); United States v. Genovese, 409 F. Supp. 2d 253 (S.D.N.Y. 2005) (trade secrets involving Microsoft Corporation's computer systems, Windows NT 4.0 and Windows 2000); United States v. Krumrei, 258 F.3d 535, 536 (6th Cir. 2001) (trade secrets belonging to company that developed new process for applying hard coatings to the laminate contact surfaces of caul plates); United States v. Hsu, 155 F.3d 189, 191-92 (3d Cir. 1998) (trade secrets related to Taxol, an anti-cancer drug produced by Bristol-Myers); United States v. Roberts, No. 08 Cr. 0175, 2009 U.S. Dist. LEXIS 123188 (E.D. Tenn. Dec. 21, 2009) (trade secrets belonging to Goodyear); United States v. Lee, No. 5:06 CR 0424, 2009 U.S. Dist. LEXIS 24972 (N.D. Cal. Mar. 18, 2009) (trade secret developed by a semiconductor manufacturing company, which it shared with another company in the course of the fabrication of semiconductor chips).[5]

[5] In contrast to § 1832, § 1831, which is directed toward foreign economic espionage, contains no explicit language requiring that the trade secret be included in or related to a product. 18 U.S.C. § 1831; see also IP Manual at 160 (comparing § 1832 to § 1831 and recognizing that in § 1831 there is "no explicit language about being included or related to a product"); Hsu, 155 F.3d at 196 (recognizing that "unlike § 1831, § 1832 also requires that the trade secret be 'related to or included in a product that is produced for or placed in interstate or foreign commerce'"). As the Supreme Court has stated, where "Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and

Numerous commentators have similarly recognized that an item constitutes a "product" under the EEA only if it is developed or actually distributed for public use and consumption. Indeed, in an article written the year after the statute was enacted, one commentator wrote that the EEA "seems to require that the trade secret owner have actually produced or sold in commerce a product containing or using the secret." James H.A. Pooley, et al., Understanding the Economic Espionage Act of 1996, 5 Tex. Intell. Prop. L.J. 177, 200 (Winter 1997). Another commentator likewise noted that the "trade secrets must be embodied in a product in the stream of commerce." Spencer Simon, The Economic Espionage Act of 1996, 13 Berkeley Tech. L.J. 305, 315 (1998) (emphasis added); see also Rice Ferrelle, Combating the Lure of Impropriety in Professional Sports Industries: the Desirability of Treating a Playbook as a Legally Enforceable Trade Secret, 11 J. Intell. Prop. L 149, 189 (Fall 2003) ("Because trade secrets must be embodied in a product in the stream of commerce, protection is limited if the trade secret relates to a rendering of services rather than a produced ware that contains or uses the secret.").

As this legal authority makes abundantly clear, the "product" element of an EEA offense is only satisfied where the alleged trade secret is or will be embodied in an item of tangible personal property that is actually distributed to the commercial public or will be so distributed upon full development. Here, however, the allegations of the Indictment establish unequivocally that the Platform is not currently, has not ever been, and will not in the future be distributed commercially for use or consumption. Accordingly, the First Count must be dismissed for failure to state an offense.

---

purposely in the disparate inclusion or exclusion." Russello v. United, 464 U.S. 16, 23 (1983).

B. The Platform Was Not Produced For Or Placed In Interstate Or Foreign Commerce.

As detailed above, it is an essential element of the EEA that the allegedly stolen trade secret was not only related to or included in a product, but also that the subject product was produced for or placed in interstate or foreign commerce. 18 U.S.C. § 1832(a). For the reasons set forth above, the Indictment's own allegations demonstrate that the Platform, which has never been and is not intended to be commercially distributed, does not qualify as a "product" under the EEA. The Indictment also establishes unequivocally that the Platform was not produced for or placed in interstate or foreign commerce.

Although no cases have interpreted the meaning of the phrase "produced for or placed in interstate or foreign commerce" in the context of the EEA, federal courts have interpreted similar statutory phrases in other settings. For example, in Kim v. Park, No. 08 C 5499, 2009 U.S. Dist. LEXIS 51591 (N.D. Ill. June 16, 2009), the district court explained that, in the context of the Fair Labor Standards Act (the "FLSA"), 29 U.S.C. § 207, "[g]oods are produced for interstate commerce 'where the employer intends, hopes, expects, or has reason to believe that the goods or an unsegregated part of them will move . . . in such interstate or foreign commerce.'" Id. at *10 (quoting 29 C.F.R. § 776.21(a)). Thus, in Velez v. Vassallo, 203 F. Supp. 2d 312 (S.D.N.Y. 2002), another FLSA case, the court held that automobiles transported to the defendant employer's parking garages in New York City "surely epitomize 'goods or materials that have been moved in or produced for' interstate commerce." Id. at 329; see also Brennan v. Indiana, No. IP 71-C-48, 1974 U.S. Dist. LEXIS 8411 at *11-12 (S.D. Ind. May 22, 1974) ("Those who have unloaded interstate shipments and who have had any contact with goods produced outside of Indiana have handled or worked on goods in commerce."); Hodgson v. Lancaster, No. CA-6-

286, 1973 U.S. Dist. LEXIS 15398 (S.D. Tex. Jan. 15, 1973) ("Where skis are manufactured and shipped by defendant from Texas to New Mexico, Oklahoma, New York and Florida, they are goods produced for interstate commerce."). These cases make clear that, to demonstrate that a product was produced for or placed in interstate or foreign commerce, it is not sufficient simply to show that the product relates to interstate or foreign commerce; rather, the product embodying the trade secret must itself be intended to, or actually, move in interstate or foreign commerce.

That the EEA applies only to trade secrets related to or included in products that move or are intended to move in interstate or foreign commerce is confirmed by the both the Department of Justice IP Manual and the United States Attorneys' Manual. As detailed above, those manuals instruct that, to support an EEA conviction, there must be proof that the product itself was a "saleable, transportable good" that was actually sold interstate or in foreign countries (for developed products) or that was intended by the victim to be distributed and sold (for developing products). See IP Manual at 160-61; U.S. Attorneys' Manual § 9-59.100. Likewise, various commentators agree that the product embodying the trade secret must itself move or be intended to move in interstate or foreign commerce. See, e.g., Simon, supra, at 315 (stating that the "trade secrets must be embodied in a product in the stream of commerce"); Ferrelle, supra, at 189 ("trade secrets must be embodied in a product in the stream of commerce"); Pooley, supra, at 200 (the EEA "require[s] that the trade secret owner have actually produced or sold in commerce a product containing or using the secret").

Here, the Indictment's own allegations demonstrate unequivocally that, due to Goldman's intentional and deliberate efforts, the Platform itself has never moved and never will move in interstate or foreign commerce. Specifically, as explained above, the Indictment expressly

alleges that "Goldman has not licensed its trading algorithms or the Platform, and has not otherwise made them available to the public." (Indictment, ¶ 6.) Having admitted that the Platform has never been licensed, leased, sold or otherwise distributed in interstate or foreign commerce, the Indictment has failed to allege that the trade secret allegedly stolen by Aleynikov was related to or included in a product that was produced for or placed in interstate or foreign commerce. Accordingly, the First Count must be dismissed for failure to state an offense.

III. THE SECOND COUNT FAILS TO STATE AN OFFENSE UNDER THE ITSPA BECAUSE THE SOURCE CODE DOES NOT CONSTITUTE "GOODS, WARES, MERCHANDISE, SECURITIES OR MONEY."

The Second Count of the Indictment alleges that Aleynikov violated ITSPA (18 U.S.C. § 2314,) by (i) copying Goldman's proprietary computer source code for its high-frequency trading business, (ii) uploading the source code to a server in Germany, and (iii) subsequently carrying some of the source code on a laptop and flash drive to a meeting in Chicago. Section 2314 applies to any person who "transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud." Thus, in order to properly state a violation of the ITSPA, the Government must allege, among other things, that Goldman's source code is a "good, ware or merchandise" within the meaning of the statute. But, because the intangible source code Aleynikov is alleged to have taken is none of those things, the Indictment fails to properly state an offense. The history of the ITSPA, Supreme Court and Second Circuit precedent interpreting the statute, and decisions of other circuit courts of appeals, all lead to the conclusion that the source code Aleynikov is alleged to have stolen is not a "good, ware or merchandise" within the meaning of the statute.

In 1919, Congress passed the National Motor Vehicle Theft Act, 18 U.S.C. § 2312, to combat the growing problem of car thieves stealing automobiles and transporting them across state lines to avoid prosecution by local law enforcement authorities. United States v. Turley, 352 U.S. 407, 413-14 (1957). Following passage of the NMVTA, "roving criminals" continued to exploit gaps in enforcement by moving tangible property other than automobiles across state lines. Because the NMVTA by its terms did not cover such crimes, Congress acted again. In 1934, Congress passed the ITSPA to prohibit interstate transportation of stolen "goods, ware, merchandise, securities or money" having a value of more than $5,000. Id. In enacting the ITSPA, "Congress was aimed at the kind of property normally the subject of theft by gangsters and racketeers." In re Vericker, 446 F.2d 244, 248 (2d Cir. 1971).

The ITSPA does not define "goods, wares, merchandise, securities or money." The Third Circuit Court of Appeals provided the leading construction of the phrase in United States v. Seagraves, 265 F.2d 876 (3d Cir. 1995), in which the court stated that "[t]he terms 'goods, wares, merchandise' is a general and comprehensive designation of such personal property or chattels as are ordinarily a subject of commerce." 265 F.2d at 880; see also United States v. Smith, 686 F.2d 234, 240-41 (5th Cir. 1982); Leonard B. Sand, et al., 3-54 Modern Federal Jury Instructions (Criminal), Instruction 54-23, comment. While broad, this definition of the term is limited to physical objects. The Second Circuit adopted the Seagraves construction in United States v. Bottone, 365 F.2d 389, 393 (2d Cir. 1966) (Friendly, J.), and In re Vericker, 446 F.2d 244, 248 (2d Cir. 1971) (Friendly, J.).

Seagraves has been interpreted as creating a two-part test for determining whether something is a good, ware or merchandise within the meaning of the ITSPA. Smith, 686 F.2d at

241; 3-54 Modern Federal Jury Instructions – (Criminal), Instruction 54.03[2], comment. First, consistent with the dictionary definition of a good, ware or merchandise, the item in question must be tangible and in the nature of personal property or chattels. Smith, 686 F.2d at 241. As the Smith court recognized, this prong of the test is consistent with Judge Friendly's statement in Bottone that "to be sure, where no tangible objects were ever taken or transported, a court would be hard pressed to conclude that 'goods' had been stolen and transported within the meaning of § 2314." Id. (quoting Bottone, 365 F.2d at 393). Second, the Seagraves test requires a determination of "whether the personal property or chattels are ordinarily a subject of commerce." Smith, 686 F.2d at 241. Even if an item constitutes personal property or chattels, it must meet the further requirement that it is commonly bought and sold. See Vericker, 446 F.2d at 248.

The intangible source code Aleynikov is alleged to have transferred does not satisfy the first prong of the Seagraves test because it is not a "good, ware or merchandise" within the commonly understood meaning of those terms.[6] As the following analysis makes clear, the better reasoned decisions reflected in every Circuit Court of Appeals to have addressed the issue, have held that § 2314 does not apply to any form of intellectual property, such as the source code at issue. See, e.g., United States v. Brown, 925 F.2d 1301, 1307 (10th Cir. 1991).

In Dowling v. United States, 473 U.S. 207 (1985), the United States Supreme Court heard a challenge by a defendant convicted under § 2314 for distributing bootleg Elvis Presley records. 473 U.S. at 210. The question presented in Dowling was whether records that included the performance of copyrighted musical compositions, without the permission of the copyright

[6] Aleynikov does not address the second prong of the Seagraves test on this motion.

holder, should be considered "stolen, converted or taken by fraud" for purposes of § 2314. Id. at 216. Although neither the parties nor the Court questioned whether the records themselves were goods, wares or merchandise within the meaning of the statutes, the Court had occasion to note that:

> [T]hese cases and others prosecuted under § 2314 have always involved ***physical*** "goods, wares, [or] merchandise" that have themselves been "stolen, converted or taken by fraud." This basic element comports with the common-sense meaning of the statutory language: by requiring that the "goods, wares [or] merchandise be the "same" as those "stolen, converted or taken by fraud," the provision seems clearly to contemplate a ***physical identity*** between the items unlawfully obtained and those eventually transported, and hence some prior physical taking of subject goods.

Id. (emphasis supplied). The Supreme Court's statement was consistent with that of the Second Circuit, made nineteen years earlier, that "where no tangible objects were ever taken or transported, a court would be hard pressed to conclude that 'goods' had been stolen and transported within the meaning of § 2314." Bottone, 365 F.2d at 393.

Following Dowling, and based upon the plain language of the statute, most courts have read "goods, wares and merchandise" in the ITSPA to impose a tangibility requirement. In Brown, the Tenth Circuit affirmed the dismissal of an indictment that charged the defendant with violating §§ 2314 and 2315 based on allegations that he transported stolen computer source code from Georgia to New Mexico. 925 F.2d at 1302. The government did not assert that the defendant took a physical object from the company and admitted that it could not prove that the defendant made a copy of the source code using the company's hard disk, or that he stole from the company the hard disk containing the source code. Id. at 1305. The trial court dismissed the indictment on the ground that the computer program itself was not a "good, ware or

merchandise" within the ambit of either statute. 925 F.2d at 1302. Based upon the rationale in Dowling, the trial court ruled that the source code was not the type of property contemplated by the phrase "goods, wares or merchandise." Id. at 1307. On appeal, the Brown court held that purely intellectual property does not fit within that category and that "the computer program itself is an intangible intellectual property, and as such, it alone cannot constitute goods, wares, merchandise, securities or moneys which have been stolen, converted or taken within the meaning of §§ 2314 or 2315." Id. at 1307-08. The Brown court also found that the government's broader reading of the statute was unsupported by its language and that even if that were less than apparent, criminal statutes should be resolved in favor of lenity. Id. at 1309.

Likewise in United States v. Stafford, 136 F.3d 1109 (7th Cir. 1998), the Seventh Circuit considered a defendant's challenge to his conviction under § 2314 for transmitting across state lines "Comdata codes." As Judge Posner explained, the codes were a series of numbers that truckers used to acquire cash while on the road by obtaining the numbers from their employers, writing them down on a "comcheck," and cashing them like a check. 136 F.2d at 1111, 1114. The government in Stafford conceded that the codes were not securities or money, but argued that they were goods, wares or merchandise. Id. at 1114. The Seventh Circuit rejected this argument, holding that the Comdata codes were merely information that lacked any physical form. As Judge Posner explained:

> The sequences have no value in themselves; they are information the possession of which enables a person to cash a check. If this information comes within the statutory terminology of goods, wares, or merchandise, then so does a tip phoned by a crook in Chicago to one in San Francisco that by posing as a police officer he learned that Wells Fargo bank in San Francisco is poorly protected and so can be knocked off easily. . . . The Comdata code has to be "goods, wares, [or] merchandise" to come within the statute. It is none of those things.

Id. at 1114-15. Accordingly, the Seventh Circuit found that the defendant was entitled to be resentenced. See also United States v. Martin, 228 F.3d 1, 13 (1st Cir. 2000) (recognizing that "intangible, 'purely intellectual' property does not fall within the auspices of § 2314.") (citing Brown, 925 F.2d at 1307-08 & n.14).

In this case, as in Dowling, Brown and Stafford, there is no physical good, ware or merchandise that is alleged to have been stolen, converted or taken by fraud by Aleynikov. The Government charges Aleynikov with stealing "Goldman's proprietary computer source code for Goldman's high-frequency trading business." (Indictment, ¶ 18.) But this is "purely intellectual property" that does not meet the statutory definition of "goods, wares or merchandise." Brown, 925 F.2d at 1307-09. Here, as in Brown, the Government does not assert that Aleynikov took a physical item from Goldman, that he made a copy of the source code using Goldman's hard disk, or that he stole from Goldman a hard disk or physical file containing the source code. Id. at 1305; cf. Bottone, 365 F.2d 393 (finding that stolen papers describing a manufacturing process were goods).

Lower court decisions that have found or suggested that the ITSPA reaches purely intangible property cannot be squared with the plain language of the statute or the decisions in Dowling, Bottone, Brown or Stafford. Compare United States v. Riggs, 739 F. Supp. 414, 417, 420 (N.D. Ill. 1990) (holding that a defendant violated § 2314 by downloading proprietary information onto a home computer and then posting it on a bulletin board) with Brown, 925 F.2d at 1308-09 (observing that the statutory interpretation espoused by Riggs is erroneous in light of Dowling's focus on physical goods, wares or merchandise that themselves have been stolen, converted or taken by fraud) and Pooley, supra, at 183 ("An analysis of the two decisions

strongly suggests that Brown, and not Riggs, was correctly decided.").

In United States v. Farraj, 142 F. Supp. 2d 484, 488 (S.D.N.Y. 2001), for example, Judge Marrero relied on Riggs to find that an 80-page excerpt of a trial plan was a "good" within the meaning of § 2314 when a paralegal working for the law firm of Orrick, Harrington & Sutcliffe LLP emailed it to opposing counsel in a tobacco class-action suit in the hopes of selling the entire plan. Id. at 486. The court echoed the concern expressed in Riggs that "reading a tangibility requirement into the definition of 'goods, wares or merchandise' might unduly restrict the scope of § 2314." Id. at 489 (quoting Riggs, 739 F. Supp. at 422). Accordingly, the Court upheld the indictment. To the extent Farraj is read for the proposition that an intangible item can be a "good" within the meaning of § 2314,[7] it is not consistent with Bottone, Dowling, or Brown, and improperly expands the scope of § 2314, which was not crafted to apply to electronic transmission of intellectual property.[8] As the Brown court held, "the element of physical 'goods, wares, or merchandise' in sections 2314 and 2315 is critical. The limitation which this places on the reach of the Interstate Transportation of Stolen Property Act is imposed by the statute itself,

---

[7] In United States v. Kwan, No. 02 Cr. 241 (DAB), 2003 U.S. Dist. LEXIS 8423 (S.D.N.Y. May 20, 2003), Judge Batts cited Farraj with approval for that proposition. Id. at **6-8. Kwan, however, involved the theft of "documents and computer diskettes containing confidential pricing and contract information," id. at *10, which are tangible items that fall squarely within the Seagraves and Bottone line of cases.

[8] To the extent Farraj, states that Brown misapplied Dowling, it is mistaken. As the legislative history of the EEA reveals, Congress was well aware of the Dowling and Brown decisions and never indicated that Brown misapplied Dowling or was otherwise wrongly decided in holding that the ITSPA was not intended to cover purely intellectual property. Rather, as discussed above, Congress responded to concerns about theft of intellectual property by enacting the EEA. See Crandon v. United States, 494 U.S. 152, 168 (1990) (under the rule of lenity, any ambiguities in a statute must be resolved in the defendant's favor "unless and until Congress plainly states that we have misconstrued its intent.").

and must be observed." Brown, 925 F.2d at 1308-09.

As numerous courts and commentators have remarked, the ITSPA is a Prohibition era statute that did not foresee — and did not attempt to prohibit — the transmission of intangible property. As the Third Circuit noted in Hsu, the ITSPA "was drafted at a time when computers, biotechnology, and copy machines did not even exist," and the case law casts serious doubt on whether the ITSPA applies to the type of intangible information involved in modern corporate espionage schemes. 155 F.3d at 194-95 & n.6 (quoting S. Rep. No. 104-359, at 10 (1996)); see also Stafford, 136 F.3d at 1114-15 ("Given the statute's age . . . and wording, and the principle that the definition of federal crimes is a legislative rather than a judicial function — a principle that places some limits on creative judicial interpretations of federal criminal statutes . . . we don't think the first paragraph of section 2314 will stretch this far.") (citations omitted).

Indeed, the impetus for passage of the EEA was Congress's understanding that the ITSPA applied only to theft of physical items. As Congress found, based upon the testimony of then FBI Director Louis Freeh:

> The principal problem appears to be that there is no federal statute directly addressing economic espionage or which otherwise protects proprietary information in a thorough, systematic manner. The statute that federal prosecutors principally rely upon to combat this type of crime, the Interstate Transportation of Stolen property Act (18 U.S.C. § 2314), was passed in the 1930s in an effort to prevent the movement of stolen property across State lines by criminals attempting to evade the jurisdiction of State and local law enforcement officials. That statute relates to "goods, wares, or merchandise." Consequently, prosecutors have found it not particularly well suited to deal with situations involving "intellectual property," property which by its nature is not physically transported from place to place. Courts have been reluctant to extend the reach of this law to this new type of property.

H.R. Rep. No. 788, 104th Cong., 2d Sess. 6-7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4025.

In enacting the EEA, Congress expressly stated its intent "to ensure that the theft of intangible information is prohibited in the same way that theft of physical items [is] protected." S. Rep., No. 104-359, 1996 WL 497065 (Leg. Hist.) at *15. See Simon, supra, at 305-06 ("The EEA was passed to fill a large hole in trade secret law that had been enlarged by the emergence of new information technologies. Prior to passage of the EEA, most federal trade secret theft cases were prosecuted . . . under the Interstate Transportation of Stolen Property Act, which was not designed nor intended to apply to intellectual property.") (footnote omitted); Pooley, supra, at 185.

In the wake of Dowling and Brown, Congress could have opted to amend the ITSPA to expressly include trade secrets within the statute's ambit, just as it previously amended the statute in 1934 to include tangible property other than automobiles. Congress chose not to take that course. Instead, it enacted an entirely new statute, the EEA — which, as the Department of Justice acknowledges, is itself "not intended to criminalize every theft of trade secrets for which civil remedies may exist under state law." U.S. Attorneys' Manual, § 9-59-100. For the reasons stated in Section II, supra, the EEA does not cover the conduct of which Aleynikov stands accused.

In sum, because the "proprietary computer source code for Goldman's high-frequency trading business" does not constitute "goods, wares, merchandise, securities or money" within the meaning of the ITSPA, the Second Count of the Indictment should be dismissed.

IV. THE THIRD COUNT FAILS TO STATE AN OFFENSE UNDER THE CFAA BECAUSE THE INDICTMENT MAKES CLEAR THAT ALEYNIKOV HAD AUTHORITY TO ACCESS, AND DID NOT EXCEED HIS AUTHORIZED ACCESS TO, GOLDMAN'S COMPUTER CODE.

The CFAA imposes criminal liability on any person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C).[9] Congress enacted the CFAA "to create a cause of action against computer hackers (e.g., electronic trespassers)." Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (quotation marks omitted). The proscribed conduct is analogous to that of "breaking and entering" rather than using a computer in committing an offense. Id. at 965.

Although the statute does not define "without authorization" or "authorization," it does define "exceeds authorized access" as "to access a computer with authorization and to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The legislative history of the CFAA reflects that Congress expected that persons who accessed a computer without authorization were likely to be outsiders and that persons who exceeded authorized access were likely to be insiders, such as employees. Shamrock, 535 F. Supp. 2d at 966.

As Judge Kaplan noted in a recent decision, courts have interpreted the CFAA's prohibitions in different ways. Orbit One Commc'ns, Inc. v. Numerex Corp., No. 08 Civ. 0905, 2010 U.S. Dist. LEXIS 36609, at *26 (S.D.N.Y. Mar. 12, 2010). Some courts apply agency law

[9] The CFFA also permits "[a]ny person who suffers damage or loss by reason of a violation of this section [to] maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

principles to the CFAA and hold that an employee who misappropriates information from his employer's computer system or accesses it for an improper purpose violates the CFAA. Id. at **26-27 & n.65 (citing, inter alia, International Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) ("[The employee's] breach of his duty of loyalty terminated his agency relationship (more precisely terminated any rights he might have claimed as [his employer's] agent — he could not by unilaterally terminating any duties he owed his principal gain an advantage!) and with it his authority to access the laptop, because the only basis of his authority had been that relationship.") and Caylon v. Mizuho Secs. USA, Inc., No. 07 Civ. 2241, 2007 U.S. Dist. LEXIS 66051, at *4 (S.D.N.Y. Sept. 5, 2007) (Owen, J.).) Other courts, including Judge Kaplan in Orbit and Judge Seybert in Jet One Group, Inc. v. Halycon Jet Holdings, Inc.. No. 08 Civ. 3980, 2009 U.S. Dist. LEXIS 72579 (E.D.N.Y. Aug. 14, 2009), "have disagreed, holding that the CFAA's prohibition of 'improper' access does not encompass an employee's misuse or misappropriation of information that the employee has lawfully accessed." Orbit, 2010 U.S. Dist. LEXIS 36609, at **26-27 & n.66 (citing cases.)

The narrower reading of the CFAA endorsed by Judge Kaplan and Judge Seybert comports with the plain language of the statute, the legislative history, and principles of criminal statutory construction.[10] See, e.g., United States v. Plaza Health Labs., 3 F.3d 643 (2d Cir. 1993) (statutory ambiguities must be resolved in the defendant's favor under the rule of lenity). First, with respect to the plain statutory language, as Judge Kaplan explained, while the CFAA expressly prohibits access without authorization and exceeding authorized access, it does not expressly prohibit misappropriation of information to which an employee was given access and

[10] As Judge Kaplan noted in Orbit "[t]he Second Circuit has not addressed the issue squarely." 2010 U.S. Dist. LEXIS 36609, at *26.

which the employee lawfully obtained. Orbit, 2010 U.S. Dist. LEXIS 36609, at **27-28. Moreover, the statute, read as a whole, indicates a congressional intent to prohibit unauthorized access and not an employee's misuse of information that he or she was entitled to access or obtain. Id. at *28.

For example, as Judge Kaplan noted, the statute's damages definitions are "consistent with the CFAA's prohibition against hacking", conduct that epitomizes unauthorized access. Id. at **28-29 & ns. 69 and 70 (citing 18 U.S.C. § 1030(e)(8) and 18 U.S.C. § 1030(e)(11). On the other hand, the damages definitions are inconsistent with a broader interpretation in that, as the Second Circuit held in Nexan Wires S.A. v. Sark-USA, Inc., 166 Fed. Appx. 559 (2d Cir. 2006), the CFAA does not permit recovery for competitive harm suffered as a result of misuse or misappropriation. Id. at **29-30.

Second, the legislative history of the CFAA likewise militates in favor of a narrow interpretation, as it "confirms that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information." Shamrock, 535 F. Supp. 2d at 966. The court in Shamrock explained:

> By enacting this amendment, and providing an express definition for "exceeds authorized access," the intent was to 'eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend,'" thereby "remov[ing] from the sweep of the statute one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization."

Id. at 966 (quoting Int'l Ass'n of Machinists & Aero. Workers v. Werner-Matsuda, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005) (quoting S. Rep. No. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479)).

Third, the rules of criminal statutory construction support a narrow reading of the CFAA. Under the rule of lenity — a manifestation of the fair warning requirement — ambiguity in a criminal statute must be resolved so "'as to apply it only to conduct clearly covered.'" Orbit, 2010 U.S. Dist. LEXIS 36609, at *30 * n.76 (quoting United States v. Velastegui, 199 F.3d 590, 593 (2d Cir. 1999)). Judge Kaplan noted that "[i]t would be imprudent to interpret the CFAA, in a manner inconsistent with its plain meaning, to transform the common law civil tort of misappropriation of confidential information into a criminal offense." Id. at *30.

In addition to Orbit, Jet One and Shamrock, numerous other courts have interpreted the CFAA narrowly. See, e.g., LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130-36 (9th Cir. 2009); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 933-36 (W.D. Tenn. July 11, 2008); Consulting Prof'l Res., Inc. v. Concise Tech. LLC, No. 09 Civ. 1201, 2010 U.S. Dist. LEXIS 32573, at **10-19 (W.D. Pa. Mar. 9, 2010); United States v. Nosal, No. C 08-0237, 2010 U.S. Dist. LEXIS 24359, at **20-21 (N.D. Cal. Jan. 6, 2010).

Under the appropriate narrow construction of the CFAA, the Indictment fails to state an offense. The Indictment asserts that Goldman limited "access to the high-frequency trading system's source code only to Goldman's employees who had reason to access that source code, such as the programmers working on the system." (Indictment, ¶ 8(b).) The Indictment concedes — indeed emphasizes — that Aleynikov was one such person: "For approximately two years, ALEYNIKOV was employed by Goldman to develop and maintain some of the computer

code used to operate Goldman's high-frequency trading business." (Id., ¶ 3.) The Indictment further asserts that "[t]hroughout his employment at Goldman, ALEYNIKOV was a member of a team of computer programmers responsible for developing and improving certain aspects of the Platform related to Goldman's high-frequency trading on equities markets." (Id., ¶ 9.) As such, according to the Indictment's own terms, Goldman permitted Aleynikov to access the source code. The Indictment therefore cannot charge that Aleynikov exceeded his access within the meaning of the statute.

Significantly, the Indictment does not assert that Goldman ever rescinded its permission to Aleynikov to access the portion of the computer containing the source code — either on the last day of his employment or at any prior time. Nor does the Indictment assert that in accessing a portion of the computer system he had permission to access, Aleynikov used that access to obtain or alter information in the computer that he was not entitled to obtain or alter. Further, the Indictment does not assert that Aleynikov accessed the Goldman computer network at any time after his last day of work. Absent such assertions, and in light of the assertions that Aleynikov had authorized access during the course of his employment to that portion of the Goldman computer containing the source code, the Indictment fails to state a CFAA offense. See Orbit, 2010 U.S. Dist. LEXIS 36609 at *31 (dismissing a CFAA claim on a motion for summary judgment, finding that as the company's executives, the defendants concededly were granted unfettered access to the computer system and the information residing on it, and consequently the company had failed to adduce any evidence that the defendants accessed the computer system without authorization or that they exceeded their authorized access in violation of the CFAA); Jet One, 2009 U.S. Dist. LEXIS 72579 at *16-22 (finding that plaintiff failed to state a

CFAA claim where the complaint alleged that, pursuant to his employment with the plaintiff, the defendant had access to confidential and proprietary information contained in the plaintiff's computer system and that the defendant wrongfully provided his new employer with confidential and proprietary information, including computer records); Brekka, 581 F.3d at 1135-36 (finding no violation of CFAA where the defendant used the company's computers to e-mail documents to his own personal computer because the defendant was authorized to access the computers during his employment with the company); Shamrock, 535 F. Supp. 2d at 968 (finding that company failed to state a claim under the CFAA because the defendant was initially authorized to access the computer he used as an employee of the company and the company conceded that the defendant was permitted to view the specific files he allegedly e-mailed himself); Consulting, 2010 U.S. Dist. LEXIS 32573 at *18-19 (dismissing CFAA claim for failure to state a claim where the employer admitted in the complaint that the employee had access to the confidential trade secret information and thus did not allege that the defendant accessed the computer without the company's authorization because "the reach of the CFAA does not extend to instances where the employee was authorized to access the information he later utilized to the possible detriment of his former employer").

The Indictment attempts to avoid the unauthorized/exceeds authorized access requirement by asserting that "in violation of Goldman's policies and his confidentiality agreement with Goldman, [Aleynikov] accessed a computer server maintained by Goldman and copied Goldman's proprietary computer source code for Goldman's high-frequency trading business . . . . uploaded the code to a computer server in Germany, and then downloaded it to his home computer . . . ." (Indictment, ¶ 20.) The allegation that Aleynikov later used the

information he obtained through his allegedly authorized computer access in a manner contrary to Goldman's policies and/or his confidentiality agreement with Goldman, however, is wholly irrelevant for CFAA purposes. The statute criminalizes unauthorized access, not unauthorized use. See Consulting, 2010 U.S. Dist. LEXIS 32573, at *18 ("[C]ases which focus on the employee's motive for accessing a computer or his eventual use of the information obtained misunderstand the statute to read "exceeds authorized use" instead of "exceeds authorized access.").

The recent decision in Nosal explains why Goldman's confidentiality agreement and policies concerning use of confidential information[11] are not relevant to the question of Aleynikov's alleged exceeding of his authorized access. In Nosal, the court dismissed certain counts of a superseding indictment for failure to sufficiently plead the necessary elements of a CFAA violation based upon the interpretation in Brekka. The Government asserted that there were a number of policies regulating the manner in which the defendants could access and use the computer system, and that those policies defined the extent of the defendants' access to the computer network. Nosal, 2010 U.S. Dist. LEXIS 24359, at **18-20. Therefore, the Government argued, when the defendants violated those policies, they "exceed[ed] authorized access." Id. at *20. The court rejected the argument, stating:

> An individual only "exceeds authorized access" if he has permission to access a portion of the computer system but uses that access to *obtain* or *alter* information in the computer that [he or she] is not entitled so to obtain or alter." [Id. (quoting 18 U.S.C. § 1030(e) (6) (emphasis added in Nosal).] There is simply no way to read that definition to incorporate corporate policies governing use

[11] The Goldman confidentiality agreement, as quoted in the Indictment, speaks only in terms of use, not access. (Indictment, ¶ 8(d)).

> of information unless the word alter is interpreted to mean misappropriate. Such an interpretation would defy the plain meaning of the word alter, as well as common sense. A person does not necessarily alter information on a computer when they access it with a nefarious intent. Furthermore, the government's proposed interpretation of "exceeds authorized access" would create an uncomfortable dissonance with section 1030(a)(4). Pursuant to the government's reading of the statute, an individual's intent would be irrelevant in determining whether that person accessed a computer "without authorization," but as long as the company had policies governing the use of information stored in its computer system, that same individual's intent could be dispositive in determining whether they "exceed[ed] authorized access." Finally, the government's proposed interpretation of "exceed authorized access" raises the same rule of lenity concerns with which the Ninth Circuit grappled regarding the "without authorization" prong of the statute.

Id. at **20-21.

Accordingly, the Nosal court found that to the extent that it alleged that the defendants exceeded their authorization to access the company's computer system by violating the company's confidentiality and terms of use agreement, the indictment failed to state a violation under § 1030(a)(4). Id. at *23. See also Black & Decker, 568 F. Supp. 2d at 933-36 (dismissing the CFAA claim because, although the complaint included claims that defendant breached an employee access agreement and the confidentiality agreements by allegedly disclosing his employer's trade secrets and proprietary information, the court found no facts indicating that he exceeded the access he was granted by the plaintiff or that he accessed the data without authorization).

In short, because the Indictment fails to adequately allege that Aleynikov accessed the Goldman computer without authorization and that he exceeded authorized access the Third Count must be dismissed.

CONCLUSION

For the reasons set forth above, defendant Sergey Aleynikov respectfully requests that the Court dismiss the Indictment in its entirety.

Dated: July 16, 2010
Chatham, New Jersey

Respectfully submitted,

MARINO, TORTORELLA & BOYLE, P.C.

By: s/Kevin H. Marino
Kevin H. Marino
437 Southern Boulevard
Chatham, New Jersey 07928-1488
(973) 824-9300
Attorneys for Defendant
Sergey Aleynikov